Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	CC Docket No. 97-213
Communications Assistance for	)	
Law Enforcement Act	)	

Reply Comments of the American Civil Liberties Union, Electronic Privacy Information Center and Electronic Frontier Foundation

Introduction

The American Civil Liberties Union ("ACLU") is a non-partisan organization of more than 250,000 members dedicated to preserving the freedoms embodied in the Bill of Rights. The Electronic Privacy Information Center ("EPIC") is a non-profit public interest research center that examines the civil liberties and privacy implications of new technologies. The Electronic Frontier Foundation ("EFF") is also a public interest organization devoted to protecting civil liberties in digital media.

The ACLU, EPIC and EFF respectfully submit comments in this Notice of Proposed Rulemaking ("NPRM") on implementation of the Communications Assistance for Law Enforcement Act ("CALEA")[1] to urge the Commission to exercise its conferred authority by extending the deadline for compliance with the Act to no earlier than October 24, 2000.[2]

Law enforcement has derailed the implementation process from the statute's inception, and neither the public, nor the telecommunications industry are in a position to comprehend the scope of the capacity and surveillance requirements sought by the Federal Bureau of Investigation ("FBI"). We believe that the impasse in the enactment process alone makes the implementation of CALEA impossible under the current statutory deadline of October, 1998.

Moreover, we believe that because the most pertinent issues, the actual technical standards that may be adopted by industry, are not addressed in this

[1]The Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in sections of 18 U.S.C. and 47 U.S.C.)

[2] 47 U.S.C. Section 1008(c)(2) and (c)(3). Under Section 107(c), the Commission is permitted to grant an extension for a period of time that it deems necessary for the carrier to comply with the assistance capability requirements. Id. at 1008(c)(3)(A).

NPRM, the Commission must extend the deadline for compliance to allow for the public scrutiny contemplated by CALEA.[3]

In short, we base our conclusions on the foregoing:

I. To date, the FBI has not met its public capacity notice requirements under the Act which require law enforcement to quantify the actual and maximum capacity technical needs, including projections with the number of anticipated interceptions. Industry, the public and the Congress need an accurate assessment of the capacity requirements to provide meaningful oversight and to ensure that they do not exceed the statutory scope. No implementation of CALEA should proceed without compliance with this statutory requirement.

II. Law enforcement was not permitted to dictate system design under CALEA, but has placed a choke hold on the process by repeatedly preventing the adoption of industry standards and creating a "wish list" of technically infeasible and costly requirements. In addition, it has become abundantly clear that the FBI is seeking unprecedented surveillance capabilities never envisioned by the Congress. Simply put they have consistently requested that industry provide numerous capabilities for surveillance that go far beyond the current court-authorized electronic surveillance under the provisions of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, the Electronic Communications Privacy Act of 1986 and CALEA. Thus, the Commission must engage in detailed review of this process by extending the compliance date.

III. *Congressional limitations on information subject to interception have been* disregarded. CALEA required the strengthening of privacy protections so that carriers do not intercept or disclose any information they are not authorized to. The additional surveillance features sought by the FBI contravene the Congress' intention to maintain current levels of surveillance and not expand them. We also address some incorrect assumptions in the NPRM that would expand CALEA's application. We conclude that these issues preclude "reasonably achievable" implementation of the Act.

Background on Surveillance and CALEA

Today, the revolutionary development of electronic infrastructures, that make it possible to easily communicate in a variety of ways, also make possible

---

[3]Paragraph 44, of the NPRM states in pertinent part:

Based on the ongoing nature of the standard-setting process, we conclude that it would be inappropriate at this time for us to address technical capability standards issues. Nothing in this Notice should be construed as evidence of any predisposition on the part of the Commission regarding capability standards, and we encourage the industry and law enforcement community to continue their efforts to develop the necessary requirements, protocols and standards.

new forms of government intrusion and surveillance. Additionally, the actual use of government surveillance has grown faster in recent years than ever before and in past 10 years, the number of interceptions per year has more than doubled.[4]

According to statistics released by the Administrative Office of the U.S. Courts and the Department of Justice:[5]

•the use of electronic surveillance for criminal and national security investigations increased substantially in 1996;

•court orders for electronic surveillance by state and federal agencies for criminal purposes also increased, from 1058 in 1995 to 1150 in 1996 (a nine percent increase);

•for the first time in eight years, a court denied a surveillance application;

•extensions of surveillance orders increased from 834 to 887. In all, interceptions were in effect for a total of 43,635 days in 1996.

The report also shows that the vast majority of interceptions continued to occur in drug-related cases: 71.4 percent (821 total) for drug investigations; 9.9 percent (114) for gambling; 9.1 percent (105) for racketeering; 3.5 percent (41) for homicide and assault and a few each for bribery, kidnapping, larceny and theft, and loan sharking. No orders were issued for "arson, explosives, and weapons" investigations.

Moreover, the according to the report, electronic surveillance continued to be relatively inefficient. Overall, 2.2 million conversations were captured in 1996. A total of 1.7 million intercepted conversations were deemed not "incriminating" by prosecutors. Each interception resulted in the capture of an average of 1,969 conversations. Prosecutors reported that on average, 422 (21.4 percent) of the conversations were "incriminating." Federal intercepts were particularly efficient, with only 15.6 percent of the intercepted conversations reported as "incriminating."

Notwithstanding the increase in government surveillance, in 1994, responding to FBI pressure and allegations that new technology hampers the ability to conduct electronic interceptions, the Congress enacted CALEA. The law was enacted during the final days of the 103d Congress amidst fervent opposition from the ACLU, EPIC, EFF and other concerned organizations that believed that the FBI had not substantiated the need for extraordinary government surveillance capabilities. We adhere to those views even today.

---

[4] Administrative office of the US Courts, 1996 Wiretap Report for the Period January 1 throughDecember 31, 1996, April 1997.
[5] Id.

Furthermore, the dramatic rise in the number of interceptions conducted rebuts the government claim that new technologies frustrate wiretapping abilities.

CALEA requires telephone carriers to ensure continued government interception capabilities despite changes in technologies by October, 1998. The legislative history of CALEA makes clear that the Act was intended "to balance three key policies: (1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies."[6] To maintain that balance, Congress established detailed guidelines on how industry standard setting organizations would accomplish the costly mandate of CALEA and imposed several obligations on law enforcement to facilitate the process as well.

Section 107 of CALEA, in pertinent part, provides that an industry association or a standards-setting organization will set the technical standards; the Attorney General must consult with the standards-setting organizations, with representatives of users of telecommunications equipment, facilities, and services, and with State utility commissions, "to ensure the efficient and industry-wide implementation of the assistance capability requirements."[7]

Section 107 further provides that if technical requirements are not issued by industry standards-setting organization or if any person believes any standards issued are deficient, the Federal Communications Commission may establish such requirements or standards.[8] The Commission has promulgated the current NPRM in response to an impasse in the implementation process and the failure of law enforcement to effectively cooperate and fulfill its statutory obligation in providing detailed notice of its technical capacity requirements so that industry can promulgate technical standards.

Section 50 of the NPRM states that this proceeding is being undertaken irrespective of the actual industry standard requirements to determine whether it is "reasonably achievable" to enact CALEA within its compliance period. The NPRM section 50 specifically states:

Because it is not clear whether requests for extension of time of the Section 103 compliance date will be forthcoming, we do not propose to promulgate specific rules regarding requests at this time. We propose to permit carriers to petition the Commission for an extension of time under Section 107, on the basis of the criteria specified in Section 109 to determine whether it is reasonably achievable for the petitioning carrier "with respect to any equipment, facility, or service installed or deployed after January 1, 1995" to comply with the assistance capability requirements of Section 103 within the compliance time period. We seek comment on that proposal. We also seek comment on what factors, other than those specified in Section 109 of CALEA, the Commission

---

[6] H.R. Rep. No. 103-827, 103d Cong., 2d Sess., pt. 1, at 13 (1994).
[7] 47 U.S.C. Section 1006 (a)(2).
[8] Id.

should consider in determining whether CALEA's assistance capability requirements are reasonably achievable within the compliance period.

The NPRM, section 45, sets out several statutory factors that the Commission may consider in determining whether CALEA's capability requirements are reasonably achievable within the compliance period. The legislative history of CALEA makes clear that the factors provided by Congress were "designed to give the Commission direction so that the following goals are realized: (1) Costs to consumers are kept low, so that 'gold-plating' by the industry is kept in check; (2) the legitimate needs of law enforcement are met, but that law enforcement does not engage in gold-plating of its demands; (3) privacy interests of all Americans are protected; (4) the goal of encouraged competition in all forms of telecommunications is not undermined, and the fact of wiretap compliance is not used as either a sword or a shield in realization of that goal."[9]

Our comments address these and other factors in concluding that the FCC should extend the compliance deadlines as permitted by Congress.

I. CALEA's Capacity Notice Requirements:

Section 104 of CALEA directed the Attorney General to issue a notice of capacity requirement to industry not later than one year after the law's enactment.[10] Hence the deadline for the notice was October 25, 1995. Carriers were provided with a deadline of three years after notification by the Attorney General to install capacity that meets the notification requirements. Under the timetable that Congress proposed, industry's deadline would have been October 1998.

Specifically, section 104(a)(2) requires the Attorney General to identify capacity required at specific locations, and to base the notice on the type of equipment or service involved, or by the type of carrier. In addition, it requires the Attorney General to provide a numerical estimate of law enforcement's anticipated use of electronic surveillance for 1998. The statute also defines the maximum capacity as the largest number of intercepts that a particular switch or system must be capable of implementing simultaneously. The initial capacity relates to the number of intercepts the government will need to make on the date that is four years after enactment.

By mandating the publication of numerical estimates of law enforcement surveillance activity, Congress intended CALEA's notice requirements to serve as "mechanisms that will allow for Congressional and public oversight. The bill requires the government to estimate its capacity needs and publish them in the Federal Register." Congress made it clear that "[t]he purpose behind the

[9] 140 Cong. Rec. H. 107-83 (October 4, 1994) .
[10] 47 U.S.C. 1003

provision is... to ensure that carriers receive adequate and specific notice from the Attorney General about the needs of law enforcement...".[11]

a. The First FBI Notice

In October, 1995, the FBI, operating under delegated authority by the Attorney General, issued a first proposed capacity notice. The Notice was criticized for; (1) failing to comply with the notification and public accountability provisions mandated in CALEA; and (2) failing to substantiate the proposed capacity requirements with adequate documentation.[12] Ultimately, it was withdrawn by the Bureau for these reasons.

The FBI's Federal Register notice failed to identify the "actual number of communications interceptions" that the Bureau estimates will be needed by the end of 1998. Instead, the capacity requirements were "presented as a percentage of the engineered capacity of the equipment, facilities, and services that provide a customer or subscriber with the ability to originate, terminate, or direct communications." 60 Fed. Reg. 53643.[13]

Furthermore, in EPIC's comments on the initial FBI notice, they stated: "[t]he Bureau's "percentage" approach to capacity requirements allows neither telecommunications carriers nor the public to 'know the required level of capacity.'" The percentages contained in the Federal Register notice (e.g., maximum capacity of one percent of "engineered capacity" for geographic areas falling within Category I) also engendered a great deal of public confusion concerning the Bureau's proposed requirements and their impact on the privacy of personal communications.

The confusion became readily apparent after an article appearing on the front page of November 2, 1995, New York Times interpreted the Bureau's notice as requiring "the capacity to monitor simultaneously as many as one out of every 100 phone lines." Asked about the issue at a press briefing later that day, Deputy Attorney General Jamie S. Gorelick said "there appears to be some misunderstanding or miscommunication as to the implications of what is contained in [the Federal Register] notice." In a letter to House Judiciary Committee Chairman Henry Hyde, Director Freeh asserted that, "We have not and are not asking for the ability to monitor one out of every 100 telephone lines or any other ridiculous number like that. ... Information supplied by the FBI was simply applied in a manner not intended to reach erroneous conclusions."

b. The Second FBI Notice

---

[11] H.R. Rep. No. 103-827, 103d Cong., 2d Sess., pt. 1, at 13 (1994).

[12] Comments of the Electronic Privacy Information Center, Re: Initial FBI Notification of Law Enforcement Capacity Requirements as Mandated in the Communications Assistance for Law Enforcement Act (November 1995).

[13] Id.

The FBI offered a revised NPRM in January, 1997, but has yet to publish rules as a result of the proceeding.[14] The second NPRM was also rejected by industry and privacy groups alike for requiring greater capacity for interceptions by carriers than actually required today.

The second FBI notice called for substantial increases in surveillance of both landline and wireless communications over the next ten years, with a total maximum capacity of 57,749 simultaneous intercepts to be conducted in the United States. Calculating out the percentages provided by the FBI, by 1998 the FBI anticipates an increase of 33 percent of landline interceptions and 70 percent of wireless phones. By 2004, the Bureau estimates a total increase of 74 percent in interceptions of landline phones and 277 percent in wireless phones.

The second notice also implied that every carrier serving a particular region would have to install capacity sufficient to meet the total surveillance needs for that area, even if the carrier only served a portion of the customers in the area. Such a plan would not only be cost prohibitive, but would provide for unauthorized and unnecessary capabilities.

Moreover, the second notice failed to make any distinction between the interception of call content and call-identifying information, even though this too was expressly required by Congress. From both constitutional law and privacy perspectives, this distinction is critical since the interception of call content is inherently more intrusive than the interception of call-identifying information. Any number of innocent individuals, conveying private information could be subject to unwarranted invasions by allowing call content information without court authorization. It is for this reason that CALEA limits the type of information that may be intercepted under pen register and trap and trace authority.

c. Law Enforcement is Actually Seeking Enhanced Surveillance Capabilities

It is now three years since the CALEA's enactment and to date the government has not promulgated final rules. The Bureau's refusal to provide the actual capacity requirements in its Federal Register notice denies any possibility of meaningful public oversight. Recently, the FBI has stated that it intends to promulgate a final notice January, 1998. Even if final regulations are promulgated at this late date, it will be impossible for industry to adopt technical standards accordingly under the current deadline of October 25, 1998. If the Congressional mandate for "public oversight" of the FBI's implementation of CALEA is to be realized, it is incumbent upon the Bureau to make available

[14]Second Notice of Capacity, Notice of Proposed Rulemaking, 62 FR 1902 (1997).

additional information concerning its proposed capacity requirements and then for the Commission to require sufficient time for public review.

Underscoring this point, on October 23, 1997, several representatives from the telecommunications industry testified before the Subcommittee on Crime of the Committee on the Judiciary of the House of Representatives on the implementation of CALEA. The consensus of each of the industry speakers was that the Bureau's failure to provide rules in a timely fashion has prevented CALEA's implementation.

Roy Neel, President and CEO of the United States Telephone Association stated, "[t]he FBI's delay in announcing its final capacity notice has been a significant obstacle for industry standard setting organizations. Throughout 1995 and early 1996, industry participants often postponed resolving certain issues pending the release of the capacity regulations and the equally anticipated Electronic Surveillance Interface."

Furthermore, it has become clear that the actual requirements that the FBI seeks go well beyond that authorized under CALEA. As we discuss below, we believe that the standards and the petitions submitted by industry and CDT/EFF make clear that the FBI has asked for capabilities not provided for by CALEA.

The expanded capabilities sought by the FBI, along with their non-compliance with CALEA's capacity notice requirements warrant a Commission order delaying implementation. Additionally, since this NPRM does not address the actual technical standards being considered for industry adoption, the Commission must extend the deadline for compliance pending public review.

It is entirely possible that industry and the FBI may achieve a compromise on the standards, but even if industry is strong-armed by the FBI into complying with their requests, we intend to petition the FCC to engage in through review of the issues not included in this proceeding.

II. Law Enforcement Has Prevented Industry Adoption of Authorized Standards By "Gold Plating" its Stated Needs

Congress expressly denied law enforcement agencies the authority to dictate the design of telecommunications networks under CALEA by conferring this authority to industry associations.[15] Industry has proposed several standards proposals which may be adopted in the near future. However, industry organizations have publicly acknowledged that law enforcement agencies have played an extensive role in the process and have thwarted the opportunity to adopt reasonable standards.

---

[15] 47 U.S.C. 1006.

Realizing that industry could not promulgate standards in light of the FBI resistance, on July 16, Cellular Telecommunications Industry Association petitioned the FCC to assume the authority over standards adoption. The petition indicates, the organizations were compelled to adopt FBI requests. More recently, in hearings on the implementation of CALEA before the House Judiciary Subcommittee on Crime, October 23, industry groups explained how the FBI has prevented adoption of reasonable standards. Many members of the Committee were critical of both the Act and the FBI. Rep. Bob Barr (R-GA), who chaired part of the hearing, bluntly stated that the legislation would not have passed in the Republican 104th or 105th Congresses.

A major area of contention was the FBI's demand for added features not required by the 1994 law. These include an enhanced ability to track geographical locations of cell phones, the ability to monitor conference calls when the targeted party has left, and the ability to separate out content from signaling data of packet-based communications.

The FBI's efforts to lobby against the industry designed standards during a vote on the specifications also came under fire. The Bureau organized a campaign to vote down the industry-developed standards, which was described in the hearing as "ballot stuffing." Twenty-eight police agencies filed the same 74-page ballot comments, including a sheriff in Florida who included the FBI's letter requesting that he file the comments. CTIA's Wheeler described the FBI's actions as "rolling a hand grenade under the table."

Another controversial issue was the FBI's effort, during its negotiations with the Telecommunications Industry Association (TIA) over the wiretap standard, to petition the American National Standards Institute (ANSI) to revoke the standards-settings authority of TIA after 50 years. The FBI apparently withdrew the request after several months.

Jay Kitchen, President of the Personal Communications Industry Association explained that the impasse in the CALEA process was due in large part to FBI interference. He stated:

"Unfortunately, a breakdown of monumental proportions has occurred. As of today, final standards have not been set, in large measure due to the actions of law enforcement officials. Initially, the FBI waited almost one and one-half years after the enactment of CALEA to submit its recommendations to standards setting bodies. After the submission of this list, industry representatives and the FBI were able to reach consensus on standards that provided, by PCIA's estimates, 90 percent of the capabilities that the FBI had requested. Since then, however, the FBI has held up the entire standards setting process in order to ensure that every capability on its "wish list" is made part of the standards."

Similarly, Matthew J. Flanagan, President of the Telecommunications Industry Association, stated that industry concessions to FBI demands have been rejected by law enforcement and they have been pressured to concede even more:

"During these meetings, industry made several concessions to law enforcement, agreeing to include features in the standard that many in industry were convinced were not required under CALEA. For example, law enforcement requested that it be provided with continuous information about the location of an intercept subject's cellular phone, irrespective of whether the phone was being used or not. Industry refused to provide this feature, finding that it greatly exceeded what CALEA permitted. In a compromise, however, industry agreed to provide law enforcement with the location of a cell phone at the beginning and end of each call -- even though many industry participants felt that even this compromise exceeded the scope of CALEA."

As a result of all of the concessions, the proposed industry standard goes well beyond a fair reading of CALEA and incorporates several of the additional features and capabilities requested by law enforcement prior to CALEA's passage but which were rejected by the Congress.

III Congressional Limitations on Information Subject to Interception Have Been Disregarded

Congress stated that CALEA was meant to preserve and not expand government surveillance capabilities. To guarantee that surveillance is not expanded, CALEA requires telecommunications carriers to protect user privacy and security of information they are not authorized to intercept.

Section 103 of CALEA, Assistance Capability Requirements, specifically imposes four industry requirements to protect privacy while assisting with law enforcement interceptions. Carriers are required to ensure that their systems are capable of:[16]

(1) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area...;
(2) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, **to access call-identifying information** that is reasonably available to the carrier--
(A) before, during, or immediately after the transmission of a wire or electronic communication...; and
(B) in a manner that allows it to be associated with the communication to which it pertains, **except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of title 18, United States Code), such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number);**
(3) delivering intercepted communications and call-identifying information to the government, pursuant to a court order or other lawful authorization, in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government to a location other than the premises of the carrier; and
(4) facilitating authorized communications interceptions and access to call-identifying information unobtrusively and with a minimum of interference with any subscriber's telecommunications service and in a manner that protects--
(A) the privacy and security of communications and call-identifying information not authorized to be intercepted; and

---

[16] 47 U.S.C. 1002(a)(1) -(4).

(B) information regarding the government's interception of communications and access to call-identifying information.[17] (emphasis added)

This section makes clear that Congress specifically limited the type of information that could be permissibly provided by industry to the FBI under CALEA by distinguishing between call content and call identifying information. Thus, we disagree with assumptions made in the NPRM that broaden the scope of communications information that may be intercepted. Section 20 states:

"We tentatively conclude that providers of **exclusively** information services, such as electronic mail providers and on-line services providers, are excluded from CALEA's requirements and are therefore not required to modify or design their systems to comply with CALEA....[W]e seek comment on the applicability of CALEA's requirements to **information services provided by common carriers**. We also note, however, that Congress anticipated that calling features such as call forwarding, call waiting, three-way calling, speed dialing, and the "call redirection portion of voice mail" would be subject to CALEA's requirements. We tentatively conclude that calling features associated with telephone service are classified as telecommunications services for the purposes of CALEA, and carriers offering these services are therefore required to make all necessary network modifications to comply with CALEA." (emphasis added)

Congress explicitly rejected any application of CALEA to information services including electronic mail and on-line services recognizing that interception of those communications is the equivalent of "call content" and is therefore, subject to a much higher degree of protection under the Constitution. The NPRM, however, incorrectly assumes there is a distinction between carriers that exclusively provide information services and common carriers that provide information services. There is absolutely no basis for such a distinction under CALEA. Congress did not exclude such services based on the carrier offering the services, but on the nature of the services and a recognition that content of communications has always been accorded greater protections.

Furthermore, the tentative conclusion that calling features associated with telephone services are subject to CALEA as "call identifying" information is incorrect. CALEA restricts recording or decoding of electronic impulses to dialing and signaling information that relates to call processing only. Congress explicitly rejected the inclusion of "other dialing tones that may be generated by the sender that are used to signal customer premises equipment of the recipient are not to be treated as call-identifying information."[18] Thus, the addition of these features is an expansion of current surveillance abilities and not permitted.

Not addressed in the NPRM are nearly a half-dozen other features that Bureau contends are "call identifying" features and thus subject to CALEA. As the Response Comments on the Petition for Rulemaking of the Center for Democracy and Technology and the Electronic Frontier Foundation, August 11, 1997, correctly point out, the FBI has sought the addition of the following features not considered by Congress:

---

[17] 47 U.S.C. Section 1002(a)(1).
[18] H.R. Rep. 103-827, Part I, at 21.

(1) packet switching information
(2) wireless telephone call location information
(3) packet data content delivery information
(4) multi-party monitoring information
(5) an expanded definition of call identifying information
(6) pen register information
(7) feature status messages[19]

Instead of addressing these threats to privacy, Section B of the NPRM frames the discussion of privacy protection in solely in terms of the type of record keeping procedures to be used by telecommunications carriers that conduct interceptions on behalf of law enforcement. However, Congress made clear that protecting the privacy of innocent individuals from surreptitious surveillance was of paramount importance and charged the Commission with the task of seeing to the necessary safeguards. The additional surveillance features sought by the FBI contravene Congress' intention that the law would maintain current levels of surveillance and not expand them. These issues must be addressed by the Commission before the implementation of CALEA can be accomplished and before record keeping and industry security procedures are determined.

Conclusion

Before rushing to embrace any proposals to enlarge the capability of government surveillance of its citizens, the ACLU and EPIC urge the Commission to take note of words written nearly 70 years ago -- that remain true even today. As Justice Louis Brandeis so aptly stated in Olmstead v. United States, 277 U.S. 438 (1928):

> The evil incident to invasion of the privacy of the telephone is far greater than that involved in tampering with the mails. Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential, and privileged, may be overheard. Moreover, the tapping of man's telephone line involves the tapping of the telephone of every other person whom he may call, or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wiretapping.

The expanded capabilities sought by the FBI, along with their non-compliance with CALEA's capacity notice requirements warrant serious Commission response. Congress envisioned the implementation process as an open process to ensure that law enforcement did not surreptitiously gain unprecedented surveillance capabilities. Thus, before the adoption of industry standards, there must be careful scrutinization of law enforcement's capability requirements. We believe the only way to accomplish this task is for the

[19] CDT, EFF petition provides detailed explanation of these features.

Commission to extend the compliance deadline to October 24, 2000 under the authority provided by the Congress.

Respectfully Submitted,

Barry Steinhardt, Associate Director
A. Cassidy Sehgal, William J. Brennan Fellow
American Civil Liberties Union
125 Broad Street, 18th Floor
New York, N.Y. 10004
(212) 549-2500

Electronic Privacy Information Center
666 Pennsylvania Ave., SE, Suite 301
Washington, D.C. 20003
(202) 544-9240

Electronic Frontier Foundation
1550 Bryant Street, Suite 725
San Francisco CA 94103-4832 USA
(415) 436-9333